Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1.-6. (Cancelled).

7. (New) A method implemented in a computer system, comprising:
generating a public key/private key pair;
encrypting data using the public key;
generating a protection key;
encrypting the public key using the protection key;
storing the encrypted data and the encrypted public key in a first database record;
encrypting the protection key; and
storing the encrypted protection key in a second database record.

8. (New) The method of claim 7, further comprising:
generating a symmetric key based on a unique user identifier; and
encrypting the private key using the symmetric key.

9. (New) The method of claim 8 wherein generating a symmetric key based on a unique user identifier comprises generating a symmetric key based on a user's user identification (ID), password, and nonce.

10. (New) The method of claim 8, further comprising decrypting the encrypted private key using the symmetric key.

11. (New) The method of claim 7, further comprising:
generating an integrity key;
decrypting the encrypted public key using the integrity key; and

storing the integrity key in a third database record in encrypted form.

12. (New) The method of claim 7, further comprising:
receiving a request from a requestor for access to the data;
authorizing the request based on a list of authorized requestors;
sending the requested data to the requestor if the requestor is authorized; and
refusing the request for data if the requestor is not authorized.

13. (New) A system, comprising:
a computer;
a database comprising encrypted data, the database accessible to the computer;
a key management process executing on the computer;
an encrypted public key stored in the database, the public key used to encrypt the data; and
an encrypted private key stored in the database, the private key used to decrypt the data;
wherein the key management process executing on the computer uses a first master key to encrypt the public key; and
wherein the key management process executing on the computer uses a unique user identifier to generate a symmetric key, the symmetric key used to encrypt the private key.

14. (New) The system of claim 13, further comprising:
an application process executing on the computer, the application process interacting with the key management process to access the data;

wherein the application process provides the unique user identifier used to generate the symmetric key, the symmetric key further used to decrypt the private key.

15. (New) The system of claim 14, further comprising:
a list of processes authorized to access the database;
wherein the data from the database is provided to the application process by the key management process if the list of processes authorized to access the database comprises the application process.

16. (New) The system of claim 13, wherein the key management process uses the first master key to decrypt the public key.

17. (New) The system of claim 13, wherein the first master key is stored in encrypted form in the database.

18. (New) The system of claim 13, wherein the key management process uses a second master key to decrypt the public key.

19. (New) The system of claim 18, wherein the second master key is stored in encrypted form in the database.

20. (New) The system of claim 13, further comprising:
a physical memory storing a decrypted master key;
wherein the decrypted master key is not swapped or paged out of the physical memory.

21. (New) A storage medium containing software that can be executed on a processor and that causes the processor to:
generate a public key used to encrypt data;
generate a private key used to decrypt the data;

generate a protection key used to encrypt the public key;

store the data, the public key, the private key, and the protection key in encrypted form in a database; and

generate a symmetric key used to encrypt and decrypt the private key, the symmetric key generation based on one or more unique user-ID/password pairs.

22. (New) The storage medium of claim 21, the software further causing the processor to decrypt the public key using the protection key.

23. (New) The storage medium of claim 21, the software further causing the processor to:

generate an integrity key used to decrypt the public key; and

store the integrity key in encrypted form in the database.

24. (New) The storage medium of claim 21, the software further causing the processor to:

accept a request for access to the data by a requestor;

grant the request for access to the data if a list of authorized requestors comprises the requestor; and

refuse the request for access to the data if the list of authorized requestors does not comprise the requestor.